UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ALEXYS WILLIAMSON, NICOLE DIGILIO and CHUNG SUK CRISPELL, individually and on behalf of all others similarly situated, Plaintiffs, v. NUVANCE HEALTH and HEALTH QUEST SYSTEMS, INC. d/b/a "HEALTH QUEST", Defendants.	Civil Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs, by and through their undersigned attorneys, as and for their class action complaint against defendants, allege as follows:

I. INTRODUCTION

1. Plaintiffs bring this data breach class action against defendants Nuvance Health and Health Quest Systems, Inc., as a result of defendants' failure to safeguard plaintiff's sensitive personal information and confidential health information ("Personal & Health Information"), including patient names, dates of birth, social security numbers, driver's license numbers, financial account information, payment card information, PINs and security codes, health care provider names, dates of medical treatment, treatment and diagnosis information, health insurance plan member and group numbers, Medicare health insurance claim numbers (HICNs) and health insurance claims information (the "Security Breach").

2. Plaintiff brings this class action on behalf of a Nationwide Class and a New York Subclass.

3. As a result of the Security Breach, plaintiffs and the class members are at a heightened risk of fraud and identity theft.

4. In response to the Security Breach, plaintiffs Alexys Williamson and Chung Suk Crispell purchased and enrolled in identity protection and credit monitoring services.

5. Plaintiffs have incurred, and likely will continue to incur, out-of-pocket costs to monitor their personal, financial and medical accounts to guard against identity theft, including but not limited to the purchase of identity theft protection services; credit monitoring services, credit freezes, credit reports and other protective and responsive measures to prevent and combat identify theft.

6. Upon information and belief, many of the putative class members are children for whom the risk of identity theft is particularly perilous.

II. PARTIES

7. Plaintiff Alexys Williamson is an individual residing in the County of Ulster, State of New York.

8. Plaintiff Nicole Digilio is an individual residing in the County of Ulster, State of New York.

9. Plaintiff Chung Suk Crispell is an individual residing in the County of Ulster, State of New York.

10. Defendant Nuvance Health is a not-for-profit corporation organized and existing under the laws of the State of New York with a principal place of business located at 28.

11. Defendant Health Quest Systems, Inc., d/b/a "Health Quest" is a not-for-profit corporation organized and existing under the laws of the State of New York with a principal place of business located at 1351 Route 55, Lagrangeville, New York 12540.

12. At all relevant times, defendant Health Quest operated the following hospitals: Vassar Brothers Hospital d/b/a "Vassar Brothers Medical Center" in Poughkeepsie, New York; Northern Duchess Hospital in Rhinebeck, New York; Putnam Hospital Center in Carmel, New York; and Sharon Hospital in Sharon, Connecticut

13. At all relevant times, defendant Health Quest's affiliate healthcare providers included: Health Quest Medical Practice, P.C., Health Quest Urgent Medical Care Practice, P.C., Hudson Valley Cardiovascular Practice, P.C. d/b/a "The Heart Center", Hudson Valley Emergency Medicine, PLLC, Health Quest Home Care Inc. (Certified), Health Quest Home Care Inc. (Licensed), Hudson Valley Newborn Physician Services, PLLC, Mid-Hudson Radiation Therapists. Inc., Northern Duchess Residential Health Care Facility, Inc. a/k/a "Thompson House," Physicians Network, P.C., Riverside Physical and Occupational Therapy and Speech Pathology PLLC d/b/a "Therapy Works" and Ulster Radiation Oncology Center.

14. Defendant Health Quest Systems, Inc., its hospitals, physician practices, healthcare providers and affiliates are collectively referred to herein as "Health Quest."

15. On or about April 3, 2019, defendants announced the creation of Nuvance Health by the merger of Health Quest and Western Connecticut Health Network.

16. The merger created an interstate health system network of seven hospitals and more than 2,600 physicians serving 1.5 million individuals.

17. According to defendants, the Nuvance Health network has combined revenues of more than $2.4 billion.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members,

some of whom are citizens of states diverse from defendants, and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

19. The Court has personal jurisdiction over defendants because they are organized and incorporated under New York law, maintain their principal place of business in this District, regularly transact business in this District, and the wrongful conduct alleged in this Complaint occurred in this District.

20. Venue is properly laid in this District pursuant to 28 U.S.C. §§ 1391(b) because defendants reside and conduct substantial business in this District, have caused harm to class members in this District, one or more of plaintiffs reside in this District, and defendants are subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants Collected and Stored Plaintiffs' Sensitive Personal and Confidential Health Information

21. Defendants and their affiliates offer healthcare services to patients at various hospitals, physician practices and other healthcare providers.

22. Defendants' healthcare services include the storage and maintenance of electronic data containing certain personal and health information of patients, including plaintiffs.

23. In July 2018, Health Quest learned that an unauthorized party, through a "phishing scheme," gained access to certain employee email accounts (hereinafter the "Security Breach").

24. The compromised email accounts contained sensitive personal and health information of Health Quest patients, including patient names, dates of birth, social security numbers, driver's license numbers, financial account information, payment card information, PINs and security codes, health care provider names, dates of medical treatment, treatment and

diagnosis information, health insurance plan member and group numbers, Medicare health insurance claim numbers (HICNs) and health insurance claims information.

25. According to defendants, Health Quest retained an outside cybersecurity firm to investigate the Security Breach.

26. Defendants waited until May 31, 2019 to send notices of the Security Breach to certain patients.

27. Then, on October 25, 2019, defendants determined that additional patient information may have been accessed by an unauthorized party.

28. By letter dated January 3, 2020, plaintiffs were each notified by defendant Quest Systems, Inc. ("HQ") that:

> On October 25, 2019, through our investigation of a phishing email incident, HQ determined that some of your information may have been contained in employee email accounts accessed by an unauthorized party. HQ first learned of a potential incident in July 2018, when numerous HQ employees were deceived by a phishing scheme, which resulted in certain HQ employees being tricked into inadvertently disclosing their email account credentials to an unauthorized party. Upon learning of the incident, the employee email accounts in question were secured and a leading cyber security firm was engaged to assist us to investigate this matter.
>
> As part of the investigation, HQ performed a comprehensive review of the voluminous contents of the email accounts in question to determine if they contained any sensitive information. Through this time-consuming review, which was completed on November 8, 2019, HQ determined that the information contained in the accounts may have included your name, health insurance information, and clinical information related to treatment you received at HQ or one of our affiliates.
>
> Although, to date, we have no evidence that any of your information has been misused or was in fact viewed or accessed, out of an abundance of caution, we wanted to let you know this happened and assure you we take it very seriously. We recommend that you regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately.

We regret any inconvenience or concern this may cause you. We are taking steps to help prevent a similar incident from occurring in the future, including the implementation of multi-factor authentication for email, as well as additional procedures to further strengthen and expand our security processes. We are also providing additional training to our employees regarding phishing emails and other cybersecurity issues.

If you have any questions, please call 1-844-967-1236 Monday through Friday, 9:00 a.m. to 6:30 p.m., Eastern Time.

29. On or about January 10, 2020, defendants posted the following on their website[1]:

Website Notice

Health Quest is committed to protecting the confidentiality and security of our patients' and employees' information. Regrettably, this notice concerns an incident involving some of that information.

On October 25, 2019, through our investigation of a phishing incident, we determined some patient information may have been contained in an email account, accessed by an unauthorized party. We first learned of a potential incident in July 2018, when numerous Health Quest employees were deceived by a phishing scheme. This resulted in certain Health Quest employees being tricked into inadvertently disclosing their email account credentials to an unauthorized party. The employee email accounts in question were secured and a leading cybersecurity firm was engaged to assist us in our investigation. As part of the investigation, we performed a comprehensive review of the voluminous contents of the email accounts in question to determine if they contained any sensitive information. HQ mailed some notification letters in May, 2019. Upon further investigation, HQ determined additional notices were required.

We determined emails and attachments in some employees' email accounts contained information pertaining to current and former patients and employees. The information involved varied by individual, but may include names in combination with, dates of birth, Social Security numbers, Medicare Health Insurance Claim Numbers (HICNs), driver's license numbers, provider name(s), dates of treatment, treatment and diagnosis information, health insurance plan member and group numbers, health insurance claims information, financial account information with PIN/security code, and payment card information.

We have no indication any patient information was viewed by the unauthorized person or has been misused. However, out of an abundance of caution, we began mailing letters to affected patients on January 10, 2020, and have established a dedicated call center to answer questions patients may have. If you have any

[1] *See* https://www.healthquest.org/Uploads/Public/Documents/Website%20Notice%201%2010%202020%20(1).pdf.

> questions regarding this incident, please call 1-844-967-1236, Monday through Friday, between 9 a.m. and 6:30 p.m. EST.
>
> We deeply regret any inconvenience or concern this incident may cause you. We continually evaluate and modify our practices to enhance the security and privacy of our patients' and employees' information. To help prevent something like this from happening in the future, we have implemented multi-factor authentication for email and additional procedures to further expand and strengthen security processes. We are also providing additional training to HQ employees regarding phishing emails and other cybersecurity issues.

30. At all times relevant, defendants had a duty pursuant to common and statutory law, including the Health Insurance Portability and Accountability Act of 1996 ("HIPA"), to maintain the confidentiality of plaintiffs' sensitive personal and protected health information.

31. Defendants acknowledge that their customers place a premium on privacy.

32. Health Quest provides each of its patients with a notice of its privacy practices.

33. Health Quest also advertises and maintains copies its privacy and data collection practices on its website.[2]

34. Health Quest's privacy practices state that it collects personal and health information about its customers and that its policy is to protect such information.

35. For example, defendant Health Quest's "Notice of Privacy Practices" effective July 3, 2014 pledges that patients have the right to privacy of their protected health information.

36. Said Notice of Privacy Practices states that:

> We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. . . .
> . . .
> The Law requires us to:
> - Make sure that medical information that identifies you is kept private.
> - Give you this notice of our legal duties and privacy practices with respect to medical information about you.
> - Follow the terms of the notice that is currently in effect.

[2] *See* https://www.healthquest.org/compliance/patient-rights-and-responsibilities.aspx.

37. The Notice of Privacy Practices further provides that patients shall be timely notified of a security breach:

> **INFORMATION BREACH NOTIFICATION**
>
> We will notify you in writing if we discover a breach of your unsecured health information, unless we determine, based on a risk assessment, that notification is not required by applicable law. You will be notified without unreasonable delay and no later than 60 days after discovery of the breach. Such notification will include information about what happened and what has been done or can be done to mitigate any harm to you as a result of such breach.

38. Defendant Health Quest's hospital Patient Bill of Rights also provides that "As a patient in a hospital in New York State, you have the right, consistent with law, to: . . . "Privacy while in the hospital and confidentiality of all information and records regarding your care."

39. Upon information and belief, defendant Health Quest Systems, Inc., its agents, servants, contractors, employees and affiliates were acting at all relevant times as the agents, servants, contractors, employees and affiliates of Health Quests' hospitals, physician practices and healthcare providers, and that the acts alleged herein occurred during the course of said agency, service, contract, employment and/or affiliation, and with the with express or implied permission, knowledge and consent of all defendants.

40. Upon information and belief, at all times relevant, defendant Health Quest maintained certain electronic information systems that provided access, storage and maintenance of sensitive personal and confidential health information for patients within its healthcare network.

41. At all times relevant, plaintiffs were patients of defendant Health Quest's hospitals, physician practices and/or healthcare providers.

42. At all relevant times, plaintiffs expected that their personal and health information related to their treatment at defendant Health Quest's hospitals, physician practices and/or healthcare providers would be kept confidential and not disclosed to anyone without their authorization.

43. At all relevant times, plaintiffs expected that Health Quest would adequately fund and implement data security measures to protect plaintiff's sensitive personal and confidential health information.

44. At all relevant times, plaintiffs expected that Health Quest would maintain physical, network and process security measures to ensure data protection of their sensitive personal and confidential health information, including technical and nontechnical safeguards.

45. Plaintiffs relied on defendants to maintain the privacy and confidentiality of their personal and health information.

B. Defendants Failed to Safeguard Plaintiffs' Personal & Health Information

46. The Security Breach demonstrates that Health Quest failed to ensure the confidentiality of plaintiffs' Personal & Health Information and to protect against reasonably anticipated threats to the security of such information, in violation its common law duties and statutory obligations under HIPAA, including but not limited to:

a. Failure to implement administrative policies to prevent, detect, contain and correct security violations, including intentional and unintentional uses or disclosures;

b. Failure to install and maintain controls governing use and access to electronic workstations, email, media and data;

c. Failure to install and maintain technical and physical safeguards for access control to ensure that only authorized personnel have access to sensitive personal and protected health information, including unique user IDs, passwords, Two-factor (2FA) or multi-factor verification, encryption, limiting server communications to approved IP addresses, audit logs, access reports, and security incident tracking reports of all activity on hardware and software applications;

d. Failure to conduct an accurate and thorough assessment of potential security risks and vulnerabilities, including cybersecurity attacks;

e. Failure to implement security measures to reduce risks and vulnerabilities, including unauthorized third-party access;

f. Failure to properly train workforce employees in technical and non-technical system security, including identification and prevention of third-party phishing attacks;

g. Failure to apply appropriate sanctions against workforce members who fail to comply with security policies;

h. Failure to regularly review information system records, including audit logs, access reports and security incident tracking reports;

i. Failure to mitigate any harmful effects resulting from the Security Breach, including timely investigation of the breach and immediate notification to patients.

47. Upon information and belief, the statement of defendant Health Quest that "we have no evidence that any of your information has been misused or was in fact viewed or

accessed" is a red-herring because Health Quest failed to maintain required technical safeguards that would have identified said unauthorized third-party access.

48. For example, defendant failed to implement a two-factor authentication system.

49. Defendants also failed to limit server communications to approved IP addresses or implement logging and monitoring systems to alert system administrators to intrusions.

50. These standard security measures would have prevented the Security Breach.

51. Defendants failed to timely notify patients, including plaintiffs, of the Security Breach.

52. Defendants concealed from patients, including plaintiffs, the true scope and nature of the Security Breach.

C. Plaintiffs' Injuries and Damages

53. The intentional third-party cyberattack on Health Quests' information systems (described as a "phishing" attack) compromised plaintiffs' Personal & Health Information, including patient names, dates of birth, social security numbers, driver's license numbers, financial account information, payment card information, PINs and security codes, health care provider names, dates of medical treatment, treatment and diagnosis information, health insurance plan member and group numbers, Medicare health insurance claim numbers (HICNs) and health insurance claims information.

54. In response to the Security Breach, plaintiffs Alexys Williamson and Chung Suk Crispell purchased and enrolled in identity protection and credit monitoring services.

55. As a result of the Security Breach, each of the plaintiffs are at a heightened and substantial risk of incurring loss from fraud and identity theft.

56. The compromised data leaves plaintiffs particularly vulnerable to identity theft, credit fraud, bank fraud, tax fraud, medical fraud, government benefits fraud, synthetic identity theft, child identity theft and other fraud. For example, identity thieves can use plaintiffs' Personal and Health Information to fraudulently bill for medical services, open financial accounts and loans in their names, file tax returns, apply for job under a false name, collect unemployment benefits or other governmental benefits, engage in utility services fraud, and other fraudulent identity theft activities.

57. Plaintiffs have spent and are likely to incur substantial time and expense to protect their personal, financial and medical accounts to guard against identity theft and misuse, including but not limited to the purchase of identity theft protection services, credit monitoring services, credit freezes, credit reports and other protective and responsive measures to prevent and combat identify theft.

58. In a report to Congress, the U.S. Government Accountability Office (the "GAO Report")[3] stated that identity thieves often use sensitive personally identifying information such as Social Security numbers and drivers' license numbers to open financial accounts, receive government benefits, and open credit cards in someone else's name.

59. As noted in the GOA Report, "identity theft victims can face a range of potential harm, from the inconvenience of having a credit card reissued to substantial financial losses and damaged credit ratings."

60. Moreover, the GAO Report warns that identity thieves may hold onto stolen data for "up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or poste on the Web, fraudulent use of that information may continue for years."

[3] *See* GOA Report 07-737 (June 2007) available at: https://www.gao.gov/new.items/d07737.pdf

61. As a result, victims of data breaches may face "substantial costs and inconveniences repairing damage to their credit records" for years long after the data breach, and are frequently required to spend substantial time and money to protect against identity theft.

62. In particular, the GOA Report states that: "Breaches that are the result of intentional acts—such as hacking into a server to obtain sensitive data—generally are considered to pose more risk than accidental breaches such as a lost laptop or the unintentional exposure of sensitive data on the Internet . . . ."

63. Accordingly, plaintiffs must vigilantly protect their financial and medical accounts for many years to come.

64. With access to the type of information that was accessed in the Data Breach, criminals can open accounts in victims' names; receive medical services in the victims' name; obtain a driver's license or official identification card in the victim's name but with the thief's photo; use the victim's name and Social Security number to obtain government benefits; file a fraudulent tax return using the victim's information; and give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

65. Sensitive personal and medical information is a valuable commodity to identity thieves. Cyber criminals routinely sell stolen Social Security numbers, drivers licenses, financial account data, medical information, and other sensitive personal information on the black-market; or post such information on anonymous dark websites, making the information widely available to a criminal underworld.

66. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

67. The financial consequences of medical identity theft are significant. A study by the Ponemon Institute concluded that the average cost to victims to resolve problems from medical identity theft was $13,453.38.[4]

68. The Ponemon study further found that victims of medical identity theft spend, on average, more than 200 hours of their personal time to secure their health credentials and verify the accuracy of their personal health information, medical invoices, insurance claims, etc.

69. Medical identity theft also places plaintiffs at risk of health insurance discrimination, increased premiums and improper denial of coverage.

70. As reported by the GAO, the "harms caused by exposure of personal information or identity theft can extend beyond tangible loss," including "emotional distress and reputation harm."[5]

71. The effects of child identity theft are also particularly problematic. For example, a survey by one of the major credit reporting bureaus found that 45% of children do not realize that they are the victims of identity theft until they were between 16 and 18 years old. The survey further found that 35% of child identity theft victims sought professional help for emotional distress caused by the fallout of being victims of identity theft.

72. Defendants knew or should have known of these cyber security risks and implemented industry standard policies and safeguards to protect plaintiffs' sensitive personal and protected health information.

---

[4] *See* Fifth Annual Study on Medical Identity Theft, PONEMON INSTITUTE (Feb. 2015) available at: http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

[5] *See* GOA Report 19-230 (March 27, 2019) available at: https://www.gao.gov/products/gao-19-230.

D. Declaratory and Injunctive Remedies

73. The scope and nature of the Security Breach and compromise of plaintiffs and the class members' sensitive personal and confidential health information, is within the sole knowledge, custody and control of defendants.

74. Plaintiffs seek declaratory and injunctive relief enjoining defendants from destroying, deleting or otherwise disposing of any physical and/or electronically stored information related to the Security Breach.

75. Plaintiffs further ask for declaratory and injunctive relief compelling an audit of defendants' electronic computer systems, at defendants' cost, by an independent court appointed computer forensic auditor, to determine the nature and scope of the Security Breach.

76. Plaintiffs further ask for declaratory and injunctive relief compelling defendants to provide plaintiffs with free credit monitoring and identity theft protection services.

77. Plaintiffs further ask for declaratory and injunctive relief compelling defendants to implement adequate data security safeguards to protect their sensitive personal and confidential health information and to undergo future data security audits.

78. Substantial and irreparable harm to plaintiffs and the class members has occurred and shall continue to occur unless the court issues an injunction.

79. Plaintiffs have no adequate remedy at law.

CLASS ALLEGATIONS

80. Plaintiffs incorporate by reference all of the paragraphs alleged above.

81. Plaintiffs seek certification of a class pursuant to Fed. R. Civ. P. 23 (a), (b)(2) and (b)(3) on behalf of a Nationwide Class and New York Subclass (collectively the "Classes"), defined as follows:

> **Nationwide Class**: All persons whose Personal & Health Information was compromised by the Health Quest data breach in or about July 2018.
>
> **New York Subclass**: All residents of New York State whose Personal & Health Information was compromised by the Health Quest data breach in or about July 2018.

82. Excluded from the Classes are all attorneys for the class, officers and members of defendants, any judge who sits on the case, and all jurors and alternate jurors who sit on the case.

83. Upon information and belief, the scope of the class may be further refined after discovery of defendants' and/or third-party records.

84. The exact number of members of the Classes, as identified above, is not known to plaintiffs, but upon information and belief, exceeds tens of thousands of persons, and is sufficiently numerous such that joinder of individual members herein is impracticable.

85. The members of the putative class are mutually and commonly aggrieved and the relief sought is common to the entire class and, if granted, would commonly benefit the entire class.

86. There are numerous questions of law and fact common to plaintiffs and the class, including:

a. Whether defendants owed a duty to plaintiffs and class members to take reasonable measures to safeguard their Personal & Health Information.

b. Whether defendants knew or should have known that their electronic information systems were vulnerable to cyberattacks, including "phishing" attacks.

c. Whether defendants breached their common law duty to reasonably safeguard and keep confidential the class members' Personal & Health Information;

d. Whether defendants breached their statutory duty of care, including violation of HIPAA;

e. Whether defendants' acts and omissions were willful, reckless and/or grossly negligent;

f. Whether defendants' conduct constitutes a breach of contract;

g. Whether class members lost the benefit of their bargain with defendants.

h. Whether defendants owed a duty to provide class members with timely and adequate notice of the Security Breach, and whether defendants' notice was in fact timely and adequate.

i. Whether defendants' conduct constitutes deceptive and unfair business practices;

j. Whether class members have suffered a loss of value of their Personal & Health Information.

k. Whether class members are entitled to injunctive relief compelling defendants to implement adequate data security safeguards to protect class members' Personal & Health Information;

l. Whether class members are entitled to recover actual damages, statutory damages and/or punitive damages, including the value of credit monitoring, identity theft protection services and other relief.

87. Common questions of fact and law predominate over any questions affecting only individual members of the class, including but not limited to the alleged acts and omissions and breach of defendants' legal duties set forth herein.

88. Plaintiffs' claims herein are typical of the claims of the class, in that the claims of all members of the class, including plaintiffs, depend on a showing of the acts and omissions of defendants giving rise to the right of plaintiffs to the relief sought.

89. Plaintiffs will fairly and adequately protect the interests of the respective class members in that plaintiffs have such a plain, direct, and adequate interest in the outcome of the controversy to assure the adequacy of the presentation of the issues involved herein. Plaintiffs have no interest which is adverse to any interest of the class members.

90. Plaintiffs have retained competent counsel with substantial experience litigating class claims in both state and federal court.

91. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Classes, and have the financial resources to do so. Neither plaintiffs nor their counsel have interests adverse to the Classes.

92. Class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy.

93. Absent class certification, individual litigation of the claims would be unreasonably expensive in light of the probable recoverable damages, burdensome upon the court, and would waste resources otherwise available to compensate the class.

94. Absent class certification, the claims of infant class members may never be timely addressed to the detriment and prejudice of said infants.

V. CAUSES OF ACTION

COUNT I

NEGLIGENCE (GROSS NEGLIGENCE)
(On Behalf of the Nationwide Class and New York Subclass)

95. Plaintiffs incorporate by reference all of the paragraphs alleged above.

96. Defendants, their agents, servants and employees, had a duty to protect the sensitive personal and confidential health information under their custody or control.

97. Defendants, their agents, servants and employees, owed a duty of trust and confidence to plaintiffs not to disclose their confidential personal information to unauthorized persons.

98. Defendants, their agents, servants and employees, had a duty to ensure that plaintiffs' confidential health information was kept and maintained in a secure manner to ensure data privacy and patient confidentiality.

99. Defendants, their agents, servants and employees, owed a duty to timely notify patients of the scope and nature of any data breach that compromised and/or disclosed their medical records.

100. Defendants breached the duty owed to plaintiffs and those similarly situated.

101. Defendants committed the minimum following acts and omissions of negligence in connection with the conduct and events alleged herein:

a. Defendants failed to exercise reasonable care to safeguard and protect sensitive personal data and confidential health information;

b. Defendants failed to protect against reasonably anticipated third-party cyber threats, including "phishing" attacks;

c. Defendants failed to adequately fund, implement, monitor, audit and oversee the security of their information systems;

d. Defendants failed to prevent the unauthorized access and/or disclosure of electronic patient sensitive personal data and confidential health information;

e. Defendants failed to apply reasonable policies and procedures so as to ensure data privacy and patient confidentiality;

f. Defendants failed to properly train their agents, servants and employees how to safeguard sensitive personal and protected health information.

g. Defendants failed to timely warn patients of the Security Breach;

h. Defendants concealed the true nature and scope of the Security Breach; and

i. Defendants failed to comply with industry standards in maintaining the security of sensitive personal data and confidential health information, and notifying patients that such information was compromised.

102. Defendants' conduct violated the provisions of HIPAA, including but not limited to: 45 CFR §§ 164.306(a)(1); 164.306(a)(2); 164.306(a)(3); 164.306(a)(4); 164.308(a)(1)(i); 164.308(a)(1)(ii)(D); 164.312(a)(1); 164.404(b) and 164.530(b).

103. Defendants failure to comply with applicable law and regulations, including the foregoing violations of HIPAA, constitutes negligence pre se.

104. As a direct and proximate result of defendants' negligence, plaintiffs have been injured, and said injury was foreseeable.

105. As a direct and proximate result of the foregoing, plaintiffs and the class members have been injured are entitled to damages in an amount to be determined at trial, including, but not limited to, monetary damages and expenses for identity theft protection services and credit monitoring, periodic credit reports, anxiety, emotional distress, loss of privacy, loss of value, and other ordinary, incidental and consequential damages as would be anticipated to arise under the circumstances.

106. Defendants knew or should have known, or consciously disregarded, the scope and nature of the Security Breach as described above.

107. Defendants consciously and deliberately delayed notifying patients of the Security Breach.

108. Defendants consciously and deliberately concealed the true nature and scope of the Security Breach.

109. Defendants consciously and recklessly failed to monitor the security of patient sensitive personal and confidential health information.

110. Upon information and belief, defendants concealed the risks and harm posed by the Security Breach. With their superior knowledge, defendants had a duty of disclosure which they violated.

111. The aforementioned conduct constitutes gross negligence, recklessness and/or wantonness which has been and continues to be a direct and proximate cause and/or contributing cause of the damages and injuries sustained by plaintiffs.

112. The acts of defendants have been intentional, willful, wanton, illegal and done with conscious and deliberate disregard for the health, safety and rights of plaintiffs and, as a result of the acts of defendants, plaintiffs are entitled to punitive damages.

113. Plaintiffs further seek injunctive relief compelling defendants to provide plaintiffs with identity theft protection services and credit monitoring; to implement adequate data security safeguards to protect their sensitive personal and confidential health information which remains in defendants' possession; and to undertake future independent cybersecurity audits of defendant's information security policies, practices and controls.

114. Plaintiffs seek declaratory and injunctive relief enjoining defendants from destroying, deleting or otherwise disposing of any physical and/or electronically stored information related to the Security Breach.

115. Plaintiffs further seek declaratory and injunctive relief: (1) compelling an audit of defendants' electronic computer systems; (2) compelling defendants to provide plaintiffs with identity theft protection services and credit monitoring; and (3) compelling defendants to implement adequate data security safeguards to protect plaintiffs and the class' Personal and Health Information and to undergo future data security audits.

COUNT II

BREACH OF CONTRACT
(On Behalf of the Nationwide Class and New York Subclass)

116. Plaintiffs incorporate by reference all of the paragraphs alleged above.

117. In consideration of plaintiffs' agreement to accept medical treatment and make payment for healthcare services rendered, defendants expressly and/or implicitly agreed to reasonably protect plaintiffs' sensitive personal data and confidential health information.

118. Defendants solicited plaintiffs' sensitive personal data and confidential health information with the express and/or implied understanding that defendants would safeguard said information from unauthorized third-party access.

119. Plaintiffs reasonably believed and expected, in entering into said agreements, that defendants' data security policies, practices and controls would comply with industry standards and applicable laws and regulations, including HIPAA.

120. At all times relevant, plaintiffs fully performed their respective obligations under the parties' agreements.

121. The acts and omissions of defendants constitute a breach of said express and/or implied agreements, all to the damage and pecuniary detriment of plaintiffs without any breach on the part of plaintiffs.

122. As a direct and proximate result of the foregoing, plaintiffs and the class members have been injured are entitled to damages in an amount to be determined at trial, including, but not limited to, monetary damages and expenses for identity theft protection services and credit monitoring, periodic credit reports, anxiety, emotional distress, loss of privacy and other ordinary, incidental and consequential damages as would be anticipated to arise under the circumstances.

123. Plaintiffs further seek declaratory and injunctive relief: (1) compelling an audit of defendants' electronic computer systems; (2) compelling defendants to provide plaintiffs with identity theft protection services and credit monitoring; and (3) compelling defendants to implement adequate data security safeguards to protect plaintiffs and the class' Personal and Health Information and to undergo future data security audits.

COUNT III

VIOLATION OF N.Y. GEN. BUS. LAW § 349
(On Behalf of the Nationwide Class and New York Subclass)

124. Plaintiffs incorporate by reference all of the paragraphs alleged above.

125. At all times relevant, defendants had a duty not to engage in unfair, misleading, false, or deceptive trade practices under New York General Business Law § 349.

126. Defendants as healthcare providers conduced business, trade or commerce.

127. Plaintiffs are consumers who purchased defendants' healthcare products and services were subjected to defendants' unfair, misleading, false and deceptive business practices as alleged herein.

128. Defendants' deceptive and misleading conduct and omissions included, but was not limited to the following:

a. Deceptive and misleading representations that defendants' would protect and maintain the confidentiality of plaintiffs' Personal & Health Information;

b. Deceptive and misleading representations that defendants' data security policies, practices and protocols complied with industry standards and applicable laws and regulations, including HIPAA;

c. Failing to disclose and remedy the defects in defendants' electronic information systems that defendants knew were vulnerable to cyberattack.

d. Continuing to collect and store sensitive personal and confidential health information when defendants knew or should have known of the security vulnerabilities exploited in the Security Breach;

e. Public concealment of the true nature and scope of the Security Breach; and

f. Failure to timely disclose and warn plaintiffs and the class of the Security Breach;

129. The acts and omissions of defendants described above constitute deceptive business acts or practices.

130. Defendants' conduct has injured the public interest and continues to pose a threat to the public.

131. Plaintiffs reasonably relied on defendants' deceptive and misleading representations and omissions to their detriment.

132. As a direct and proximate result of the foregoing, plaintiffs and the class members have been injured are entitled to damages in an amount to be determined at trial, including, but not limited to, monetary damages and expenses for identity theft protection services and credit monitoring, periodic credit reports, anxiety, emotional distress, loss of privacy and other ordinary, incidental and consequential damages as would be anticipated to arise under the circumstances.

133. Plaintiffs further seek declaratory and injunctive relief: (1) compelling an audit of defendants' electronic computer systems; (2) compelling defendants to provide plaintiffs with identity theft protection services and credit monitoring; and (3) compelling defendants to implement adequate data security safeguards to protect plaintiffs and the class' Personal and Health Information and to undergo future data security audits.

COUNT IV

BREACH OF CONFIDENCE
(On Behalf of the Nationwide Class and New York Subclass)

134. Plaintiffs incorporate by reference all of the paragraphs alleged above.

135. At all times relevant, defendants owed a duty of confidence to patients, including plaintiffs, to not disclose their confidential personal and health information.

136. The acts and omissions of defendants alleged heretofore constitute a breach of defendants' duty of confidence owed to plaintiffs.

137. As a direct and proximate result of the foregoing, plaintiffs and the class members have been injured are entitled to damages in an amount to be determined at trial, including, but not limited to, monetary damages and expenses for identity theft protection services and credit monitoring, periodic credit reports, anxiety, emotional distress, loss of privacy and other ordinary, incidental and consequential damages as would be anticipated to arise under the circumstances.

138. Plaintiffs further seek declaratory and injunctive relief: (1) compelling an audit of defendants' electronic computer systems; (2) compelling defendants to provide plaintiffs with identity theft protection services and credit monitoring; and (3) compelling defendants to implement adequate data security safeguards to protect plaintiffs and the class' Personal and Health Information and to undergo future data security audits.

COUNT IV

UNJUST ENRICMENT
(On Behalf of the Nationwide Class and New York Subclass)

139. Plaintiffs incorporate by reference all of the paragraphs alleged above.

140. In the alternative to the claims alleged above, plaintiff allege that have no adequate remedy at law and that defendants have been unjustly enriched to the detriment of plaintiffs.

141. Plaintiffs' payment for healthcare services conferred a monetary benefit on defendants.

142. Defendants accepted and enjoyed said benefit, including revenue and profit from the healthcare services paid by plaintiffs, which in fairness and good consciousness should not be retained.

143. Plaintiffs anticipated and defendants knew, or should have known, that said healthcare services included the protection of plaintiffs' personal and health information.

144. The payments by plaintiffs should have been used by defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices.

145. Defendants failed to implement reasonable data privacy and security practices in violations of applicable law and regulations, including HIPAA, and industry standards and best practices.

146. As a direct and proximate result of defendants' conduct, plaintiffs suffered actual damages in an amount equal to the difference in value between the healthcare services associated with the reasonable data privacy and security practices that plaintiffs paid for, and the inadequate healthcare services without reasonable data privacy and security practices that plaintiffs received.

147. Defendants should not be permitted to retain the money benefit conferred by plaintiffs because defendants failed to use that money to implement the reasonable data privacy and security practices that plaintiffs paid for and which were otherwise required by applicable statutory law, HIPAA regulations, and industry standards and best practices.

148. The acts and omissions of defendants alleged heretofore constitute unjust enrichment.

149. As a direct and proximate result of the foregoing, plaintiffs and the class members have been injured are entitled to equitable relief and disgorgement of defendants' profits, together with monetary and non-monetary damages for identity theft and credit protection, monitoring and insurance, periodic credit reports, anxiety, emotional distress, loss of privacy and other ordinary, incidental and consequential damages as would be anticipated to arise under the circumstances.

150. Plaintiffs further seek declaratory and injunctive relief: (1) compelling an audit of defendants' electronic computer systems; (2) compelling defendants to provide plaintiffs with identity theft protection services and credit monitoring; and (3) compelling defendants to implement adequate data security safeguards to protect plaintiffs and the class' Personal and Health Information and to undergo future data security audits.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs demand relief against defendants as follows:

1. Certification of this action as a class action;
2. Declaratory relief adjudicating the parties' legal rights and obligations;
3. Iinjunctive relief (1) compelling an audit of defendants' electronic computer systems; (2) compelling defendants to provide plaintiffs with identity theft protection services and credit monitoring; and (3) compelling defendants to implement adequate data security safeguards to protect plaintiffs and the class' Personal & Health Information and to undergo future data security audits;
4. Compensatory, statutory, and punitive damages; disgorgement of profits; restitution; and pre-judgment and post-judgment interest, in an amount to be determined upon trial;
5. Attorneys' fees, disbursements and costs; and
6. Such other and further relief as the Court deems just and proper.

VII. JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: February 28, 2020

Respectfully,

/s/ James R. Peluso
James R. Peluso (Bar Roll # JP2875)
DREYER BOYAJIAN LLP
75 Columbia Street
Albany, NY 12210
Telephone: (518) 463-7784
jpeluso@dblawny.com

/s/ Joseph E. O'Connor
Joseph E. O'Connor (Bar Roll # JO5185)
O'Connor & Partners, PLLC
255 Wall Street, Kingston, NY 12401
Telephone: (845) 303-8777
joconnor@onplaw.com

Attorneys for Plaintiffs